ISIP

INITIATIVE FOR STATE INFRASTRUCTURE PROTECTION

A Department of Defense Program

25 September 2003

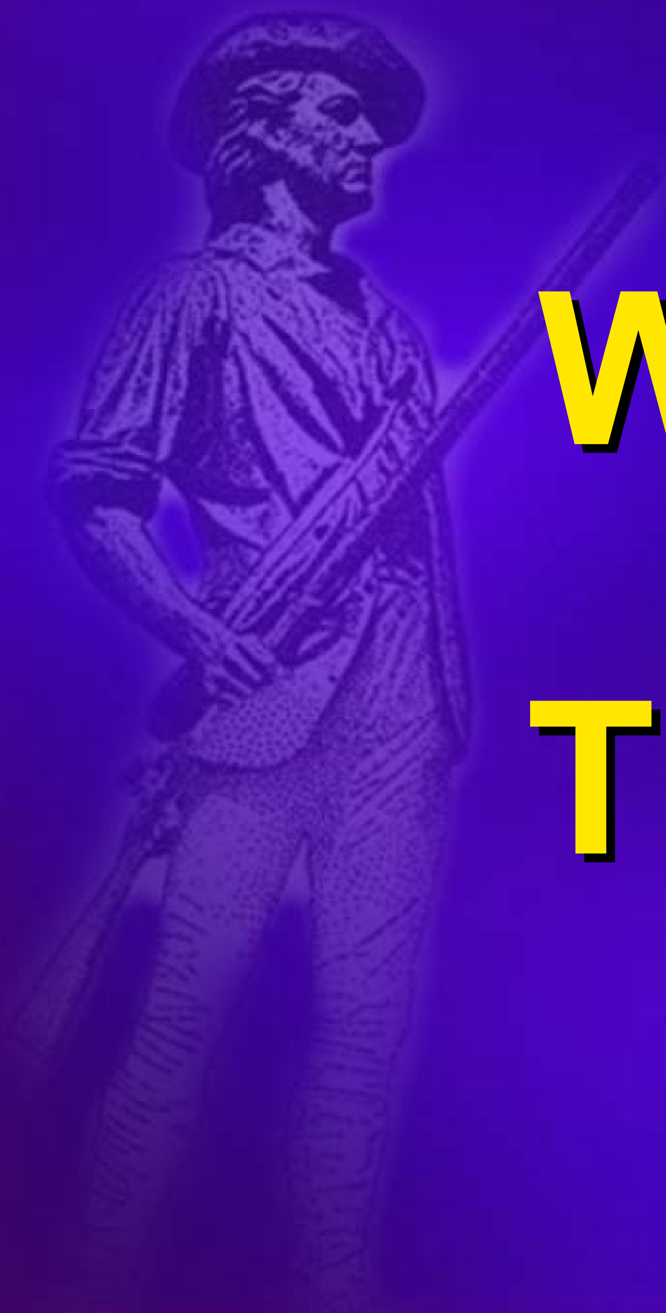
Brad L. Shere

NETCOM/9TH ASC (NETC-EST-A)

Office of the Chief Information Officer/G6

Headquarters, Department of the Army

Bradley.Shere@us.army.mil



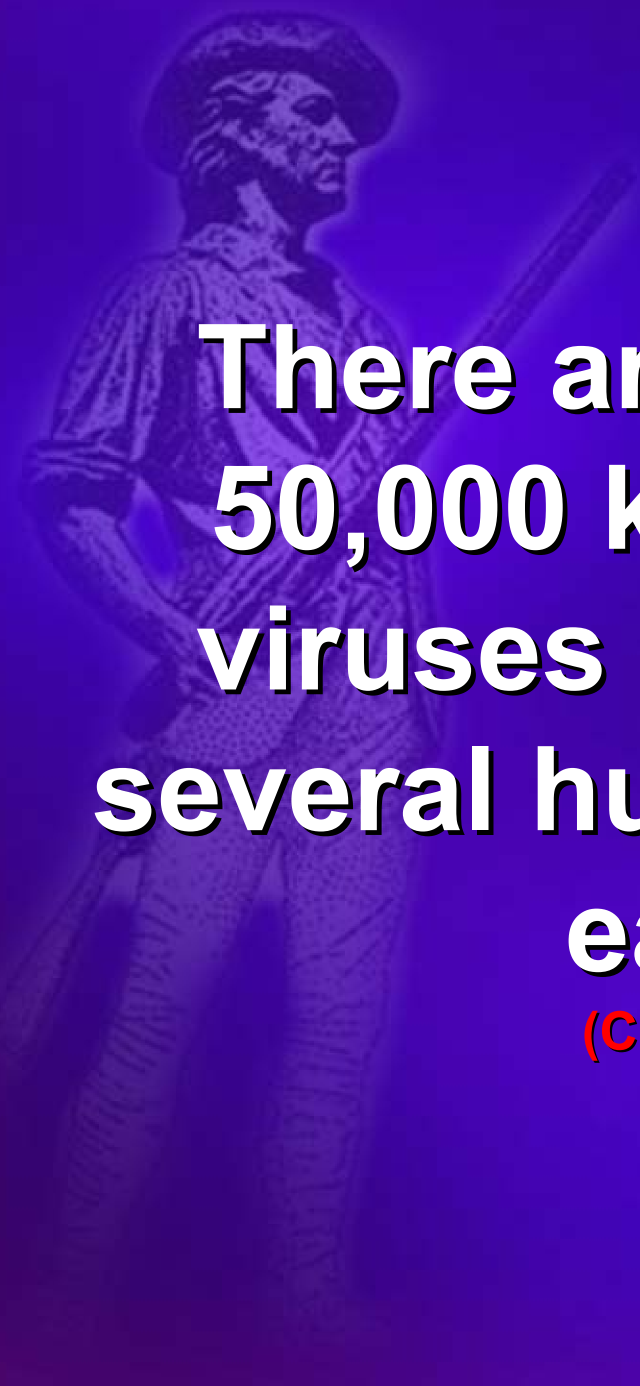
What is the Threat?

Information Warfare: The Computer as a Weapon

"In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars."

Major General Wang Pufeng (former Director of the Strategy Department, Academy of Military Science, Beijing.)

His paper was excerpted from China Military Science (Spring 1995).



There are approximately 50,000 known computer viruses in existence and several hundred are created each week.

(Computer Economics)

Exercise Eligible Receiver

Eligible Receiver was conducted in the summer of 1997 and was the first large-scale no-notice DOD exercise designed to test the ability of the United States to respond to an attack on DoD and U.S. national infrastructure.

This exercise involved a simulated attack against components of the national infrastructure (e.g., power and communications systems) and an actual "red team" attack against key defense information systems at the Pentagon, defense support agencies, and in combatant commands.

The exercise revealed vulnerabilities in DoD information systems and deficiencies in the ability of the United States to respond effectively to a coordinated attack on the national infrastructure and information systems. Poor operations and information security practices provided many red team opportunities.

Eligible Receiver discovered that 62% to 65% of all U.S. Federal computer systems had known security holes that could be exploited.

Solar Sunrise:
Dawn of a New Threat

In February 1998, hackers launched an attack against the Pentagon and MIT in what DoD called “the most organized and systematic attack to date.”

The attacks targeted network domain servers by exploiting a well-known vulnerability in the Solaris operating system.

Many passwords were obtained and attacks were conducted on key Defense Department support systems (the global transportation system, defense finance system, and medical, personnel, logistics and official unclassified email.

Solar Sunrise confirmed the findings of Eligible Receiver

Melissa Virus

Melissa is a fast-spreading macro virus that was introduced in March 1999 and was distributed as an e-mail attachment that, when opened, disabled a number of safeguards in Word 97 or Word 2000, and, if the user had the Microsoft Outlook e-mail program, caused the virus to be resent to the first 50 people in each of the user's address books.

Melissa was the first ever email-bound executable virus. Companies such as Microsoft, Intel, Lockheed Martin, and Lucent Technologies were forced to shut down their email gateways because of the large amount of email generated by the virus. It also caused the closure of e-mail systems of government agencies in both the US and UK.

David Smith was arrested one week after Melissa was introduced and later pled guilty and was sentenced to 20 months in jail and ordered to pay $5,000 in damages.

The Melissa virus caused an estimated $80 million damage to computers and systems worldwide.

VBS/Loveletter

VBS/Loveletter is an email worm was released in 2000 and infects Windows 98 and Windows 2000 systems and Windows 95 and Windows NT users can be affected if the Visual Basic scripting is enabled.

The worm comes through an email attachment with the message having the title 'I LOVE YOU'. Opening the attachment launches the worm, which then sends a message with the attachment to everyone in the address book.

The virus affected stock brokerages, food companies, media, auto and technology giants, as well as government agencies, universities and medical institutions worldwide.

It may have hit as many as tens of millions of computers, as compared with the Melissa virus, which affected about 300,000 computers in the United States. It caused between $7.8 billion and $9.6 billion in damage.

Nimda Worm

The Nimda worm was released in September 2001and has the potential to affect both user workstations (clients) running Windows 95, 98, ME, NT, or 2000 and servers running Windows NT and 2000.

Nimda is the first worm to modify existing web sites to start offering infected files for download. Also it is the first worm to use normal end user machines to scan for vulnerable web sites. This technique enables Nimda to easily reach intranet web sites located behind firewalls

Nimda infected 2.5 million computers, taking just one day to infect local area networks and individual desktops globally.

According to Computer Economics, the worldwide economic impact of the Nimda worm reached about $590 million.

Code Red Worm

The Code Red worm, released July 2001, sends probes across the Internet, looking for computers with a security weakness (a computer that has not been patched for the.ida vulnerability). The worm does little damage to the computers it infects. The danger of Code Red lies in the pressure it puts on Internet infrastructure.

Code Red is programmed to actively propagate between the 1st and 19th day of each month. On the 20th day of each month, all of the infected computers launch an attack on the server hosting the White House website to try to crash it with a flood of data and traffic.

The White House has since moved its website, so it will not be affected, but the attack will continue and may affect the overall performance of the Internet.

The worldwide labor costs associated with cleaning up the Code Red worm is estimated $2.4 billion to $2.9 billion in damage

The Klez Family

The Klez virus, released in 2002, is a mass-mailing email worm that exploits a vulnerability in Microsoft Outlook and Outlook Express in an attempt to execute itself when you open or even preview the message in which it is contained.

The worm uses random subject lines, message bodies, and attachment file names. It also can generate random email addresses by taking the "from" address and the "to" address from files on the infected computer.

Klez can infect your PC without opening an e-mail attachment. Simply clicking on an e-mail subject or previewing a message is enough to catch the virus.

The Klez Family of virus' has caused an estimated $13.9 billion damage worldwide.

SQL Slammer

Released in early 2003, SQL Slammer exploited a flaw in Microsoft Corp.'s SQL Server database software and caused damage by rapidly replicating itself and clogging the pipelines of the global data network. The program, also known as Sapphire, did not erase data or cause damage to desktop computers, but was designed to replicate itself so fast and so effectively that no other traffic could get through networks.

It only took 10 minutes for the SQL Slammer worm to race across the globe. The worm, which nearly cut off Web access in South Korea and shut down some U.S. bank teller machines, doubled the number of computers it infected every 8.5 seconds in the first minute of its appearance.

By comparison, the Code Red worm -- which came 18 months earlier -- only doubled every 37 minutes.

Economic damage from the SQL Slammer worm is already over $1 billion.
Microsoft released SQL Slammer patch 9 months earlier.

PDD 63

(Critical Infrastructure Protection)

Builds on the recommendations of the President's Commission on Critical Infrastructure Protection.

In 1997 the Commission called for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures (telecommunications, banking and finance, energy, transportation, and essential government services).

The President's policy:

Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000, by:

- **Establishing a national center to warn and respond to attacks.**

- **Building the capability to protect critical infrastructures from intentional acts by 2003.**

PDD-63 sets up a new structure to deal with this important challenge:

- *National Coordinator* whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction.

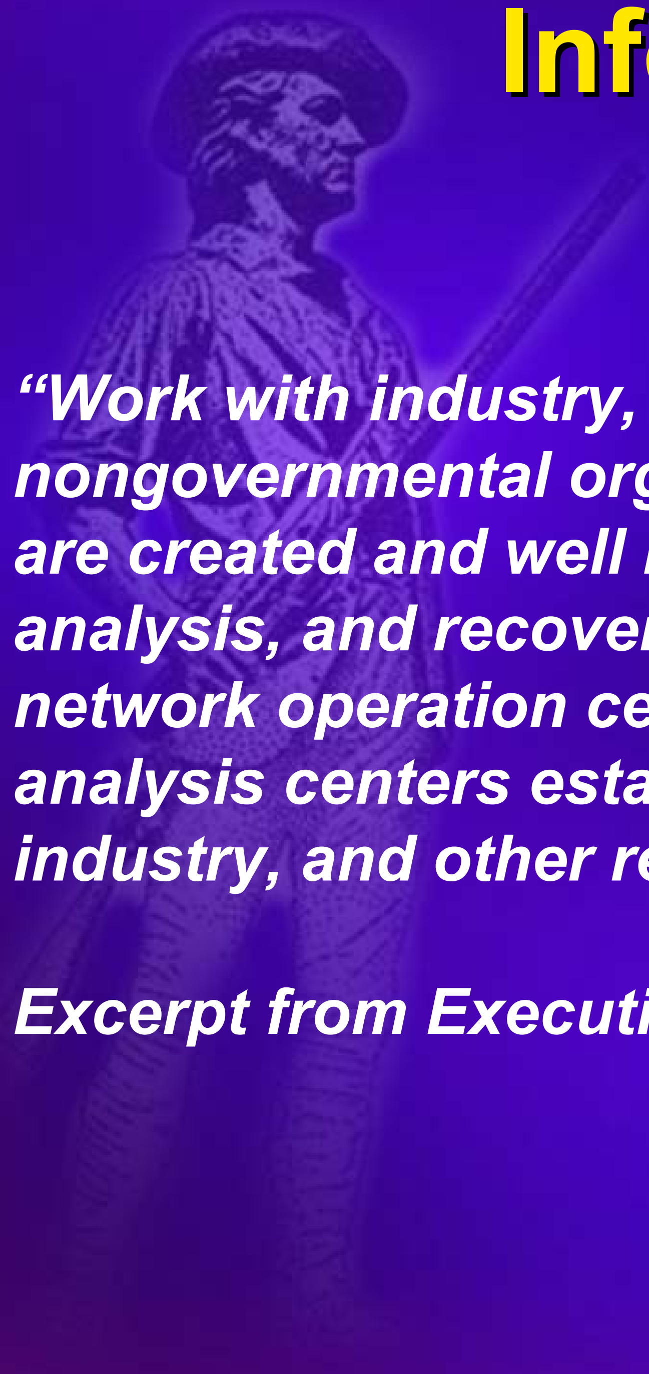
- The *National Infrastructure Protection Center* (NIPC) at the FBI which will fuse representatives from FBI, DOD, USSS, Energy, Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector.

- An *Information Sharing and Analysis Center* (ISAC) is encouraged to be set up by the private sector, in cooperation with the federal government.

- A *National Infrastructure Assurance Council* drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan.

- The *Critical Infrastructure Assurance Office* (CIAO) will provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan.

Information Sharing



"Work with industry, State and local governments, and nongovernmental organizations to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers established on a voluntary basis by industry, and other related operations centers."

Excerpt from Executive Order 13231, October 16, 2001

Background

ISIP was initially developed by the Defense Information Assurance Program (DIAP) and vetted through an interagency working group that included members from the Department of Defense (DoD), Department of Commerce, Department of Justice, and the National Infrastructure Protection Center (NIPC).

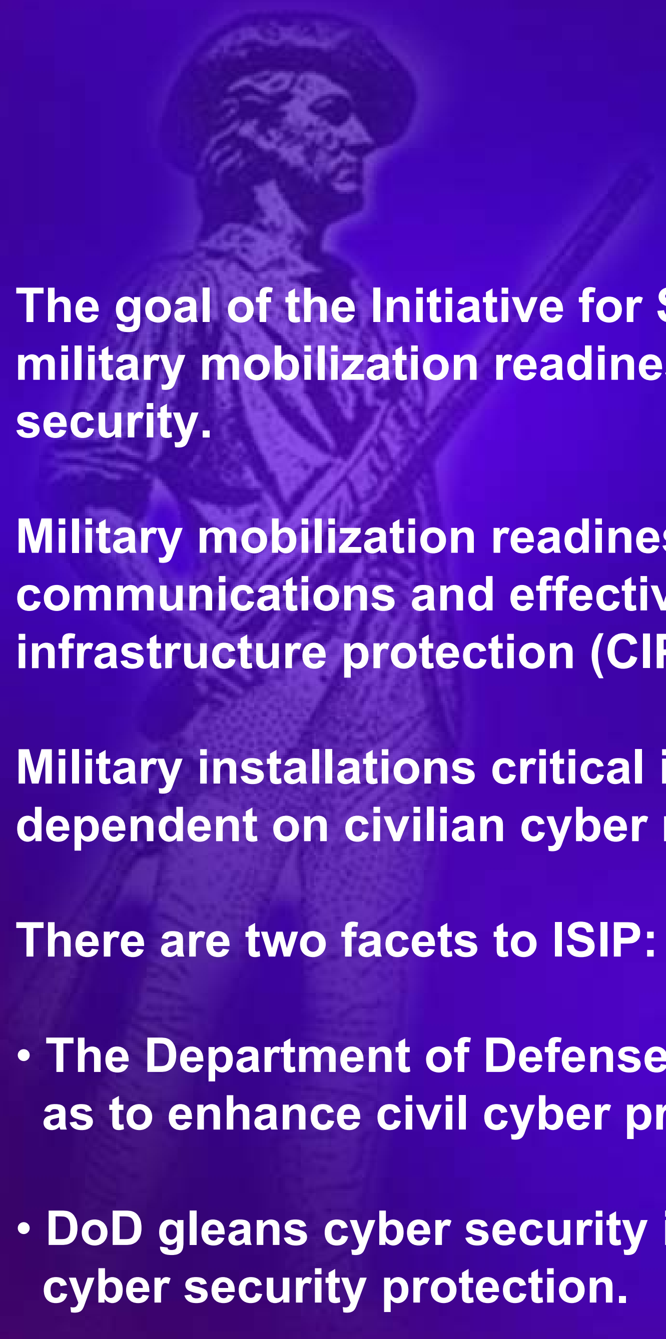
ISIP

INITIATIVE FOR STATE INFRASTRUCTURE PROTECTION

A Department of Defense Program

Robert F. Lentz, (ASD-C3I, Dir. Information Assurance) passed oversight of the ISIP program to the Department of the Army (CIO/G6) in April 2002 due to the Army’s “preeminent Homeland Security role and historical involvement with ISIP.”

ISIP Goals



The goal of the Initiative for State Infrastructure Protection (ISIP) is to assure military mobilization readiness through the enhancement of Civil cyber security.

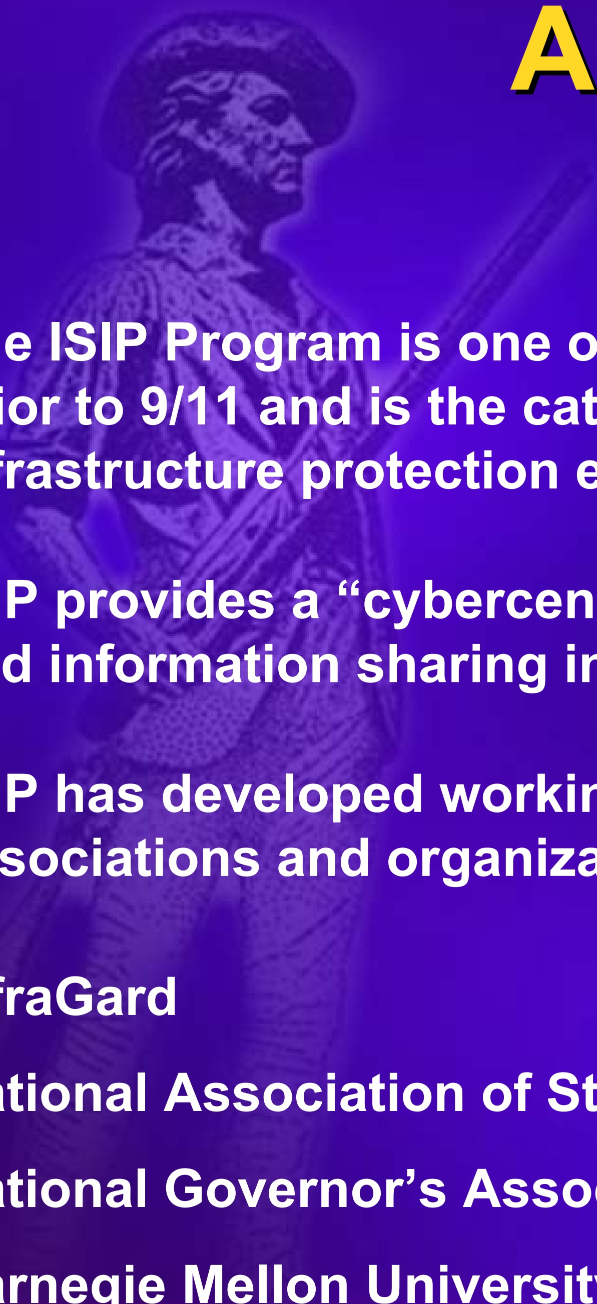
Military mobilization readiness is dependent on effective nationwide cyber communications and effective cyber military installation critical infrastructure protection (CIP).

Military installations critical infrastructure protection is significantly dependent on civilian cyber resources.

There are two facets to ISIP:

- The Department of Defense (DoD) shares cyber information resources so as to enhance civil cyber protection capabilities.
- DoD gleans cyber security information from civil sensors to enhance DoD cyber security protection.

Accomplishments



The ISIP Program is one of the few cyber security programs begun prior to 9/11 and is the catalyst to bridge DoD and state critical infrastructure protection efforts.

ISIP provides a “cybercentric” approach to vulnerability management and information sharing in terms of critical infrastructure protection.

ISIP has developed working relationships with numerous national associations and organizations:

InfraGard

National Association of State Chief Information Officers (NASCIO)

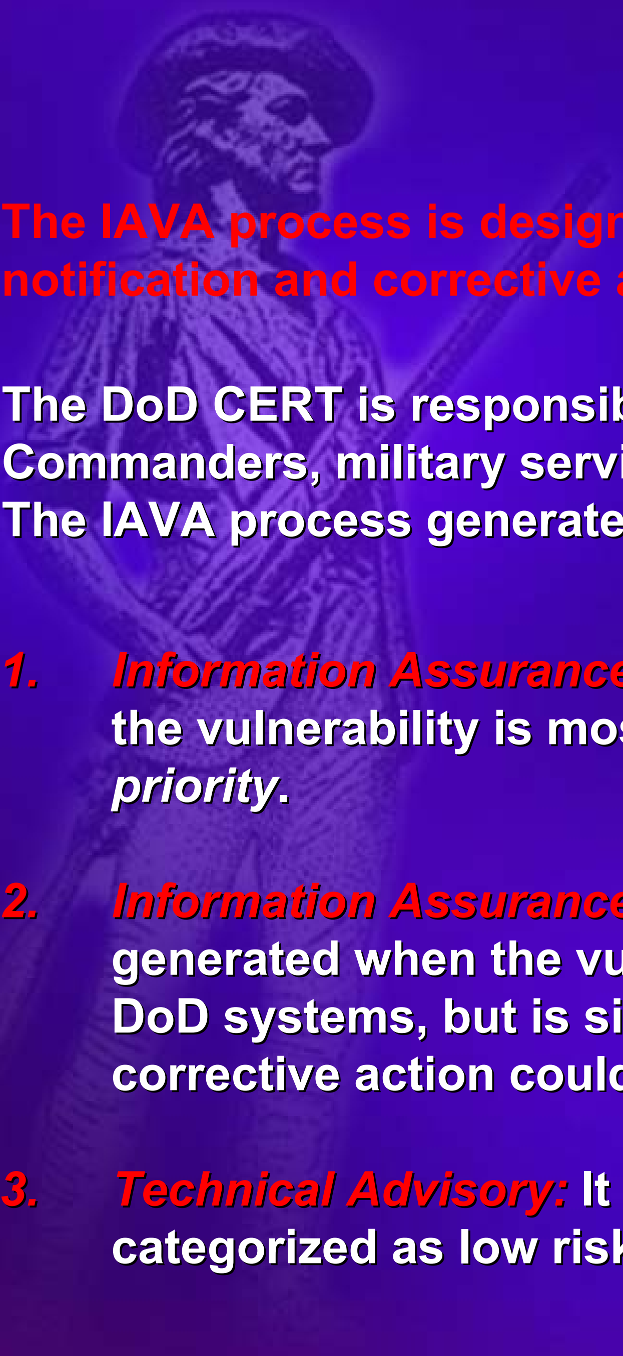
National Governor’s Association (NGA)

Carnegie Mellon University

ISIP's Foundation

- Information Assurance Vulnerability Alert (IAVA) Process
- State Infrastructure Protection Center (SIPC)
- Cyber Exercise Development

Information Assurance Vulnerability Alert (IAVA)



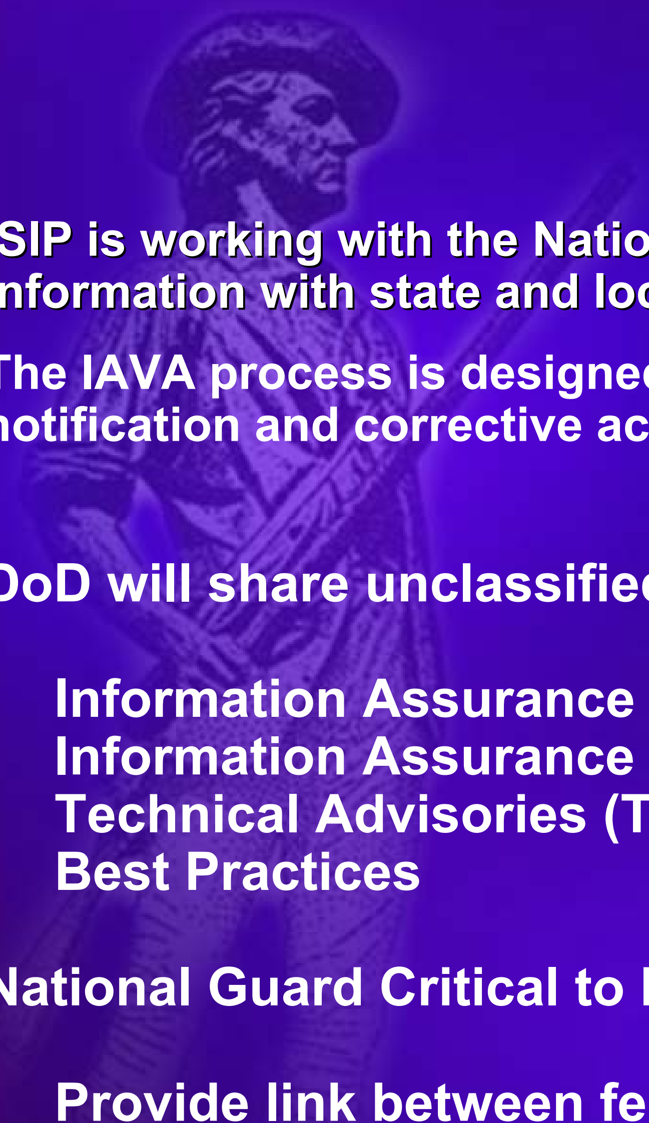
The IAVA process is designed to provide *positive control* of the vulnerability notification and corrective action process within DoD.

The DoD CERT is responsible for disseminating IAVA's to Combatant Commanders, military services, and agencies (C/S/A) points of contact. The IAVA process generates three types of notifications:

1. ***Information Assurance Vulnerability Alert (IAVA):*** **It is generated when the vulnerability is most severe and corrective action is of the *highest priority*.**

2. ***Information Assurance Vulnerability Bulletin (IAVB):*** **This bulletin is generated when the vulnerability does not pose an immediate threat to DoD systems, but is significant enough that non- compliance with the corrective action could escalate the threat.**

3. ***Technical Advisory:*** **It is generated when the vulnerability exists but is categorized as low risk.**



ISIP is working with the National Guard to share cyber security vulnerability information with state and local governments.

The IAVA process is designed to provide positive control of the vulnerability notification and corrective action process within DoD.

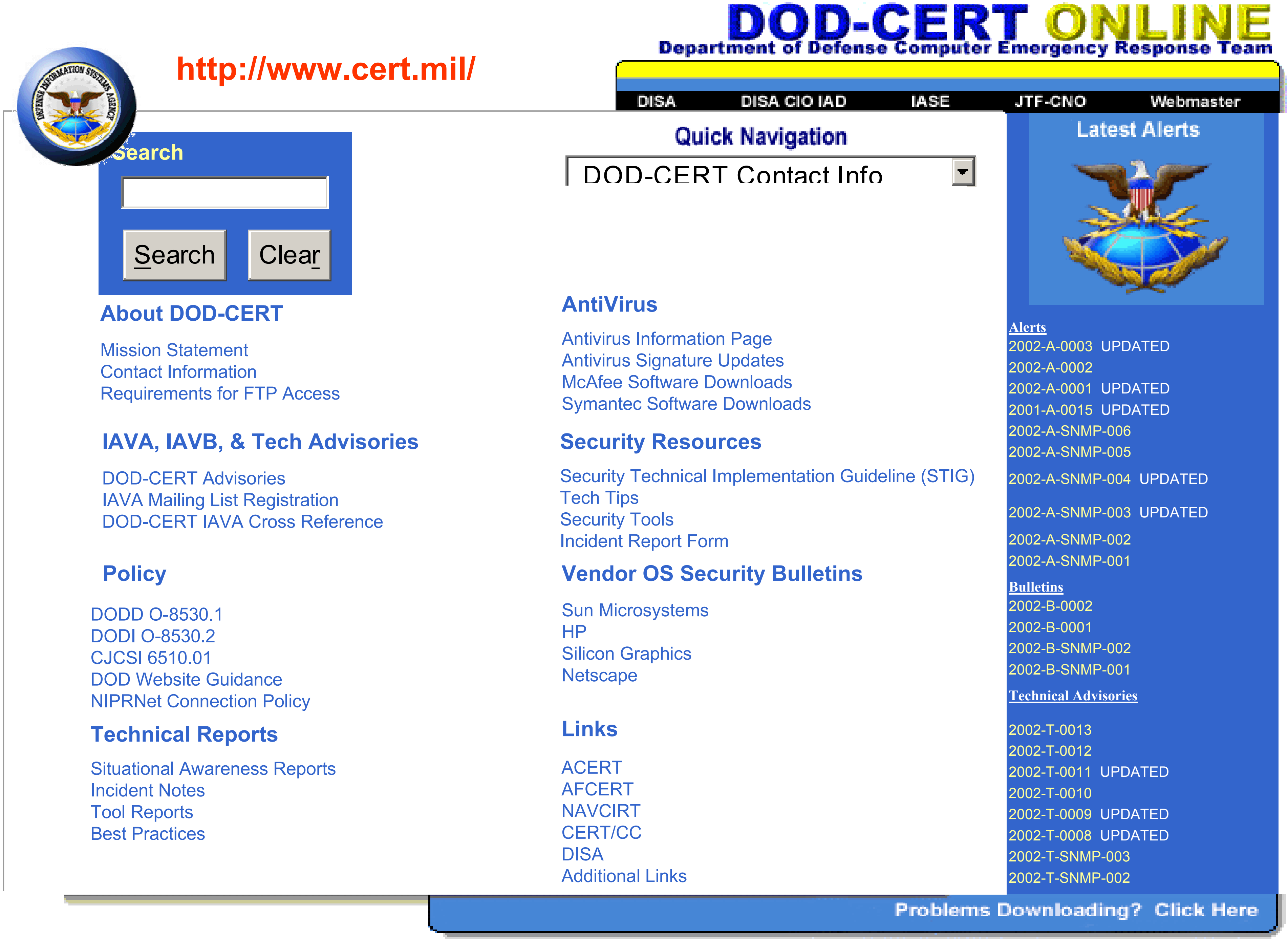
DoD will share unclassified technical information:

- **Information Assurance Vulnerability Alerts (IAVA)**
- **Information Assurance Vulnerability Bulletins (IAVB)**
- **Technical Advisories (TA)**
- **Best Practices**

National Guard Critical to Effective Sharing:

- **Provide link between federal and state governments**
- **NG already plays an integral role in most state emergency operations centers**
- **NG personnel bridge gap between public and private sectors**

http://www.cert.mil/



DOD-CERT ONLINE

Department of Defense Computer Emergency Response Team

Quick Navigation

About DOD-CERT

Mission Statement
Contact Information
Requirements for FTP Access

IAVA, IAVB, & Tech Advisories

DOD-CERT Advisories
IAVA Mailing List Registration
DOD-CERT IAVA Cross Reference

Policy

DODD O-8530.1
DODI O-8530.2
CJCSI 6510.01
DOD Website Guidance
NIPRNet Connection Policy

Technical Reports

Situational Awareness Reports
Incident Notes
Tool Reports
Best Practices

AntiVirus

Antivirus Information Page
Antivirus Signature Updates
McAfee Software Downloads
Symantec Software Downloads

Security Resources

Security Technical Implementation Guideline (STIG)
Tech Tips
Security Tools
Incident Report Form

Vendor OS Security Bulletins

Sun Microsystems
HP
Silicon Graphics
Netscape

Links

ACERT
AFCERT
NAVCIRT
CERT/CC
DISA
Additional Links

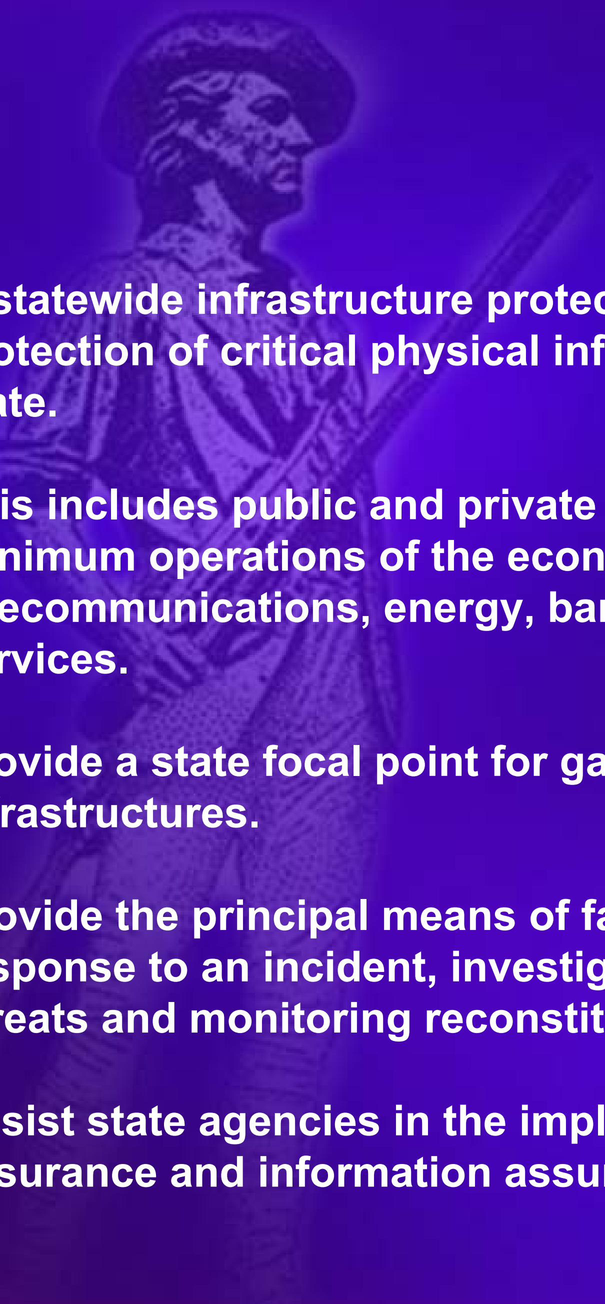
Latest Alerts

Alerts
2002-A-0003 UPDATED
2002-A-0002
2002-A-0001 UPDATED
2001-A-0015 UPDATED
2002-A-SNMP-006
2002-A-SNMP-005
2002-A-SNMP-004 UPDATED
2002-A-SNMP-003 UPDATED
2002-A-SNMP-002
2002-A-SNMP-001

Bulletins
2002-B-0002
2002-B-0001
2002-B-SNMP-002
2002-B-SNMP-001

Technical Advisories
2002-T-0013
2002-T-0012
2002-T-0011 UPDATED
2002-T-0010
2002-T-0009 UPDATED
2002-T-0008 UPDATED
2002-T-SNMP-003
2002-T-SNMP-002

State Infrastructure Protection Center (SIPC)



A statewide infrastructure protection center concept is to coordinate and integrate the protection of critical physical infrastructure and information infrastructure for the state.

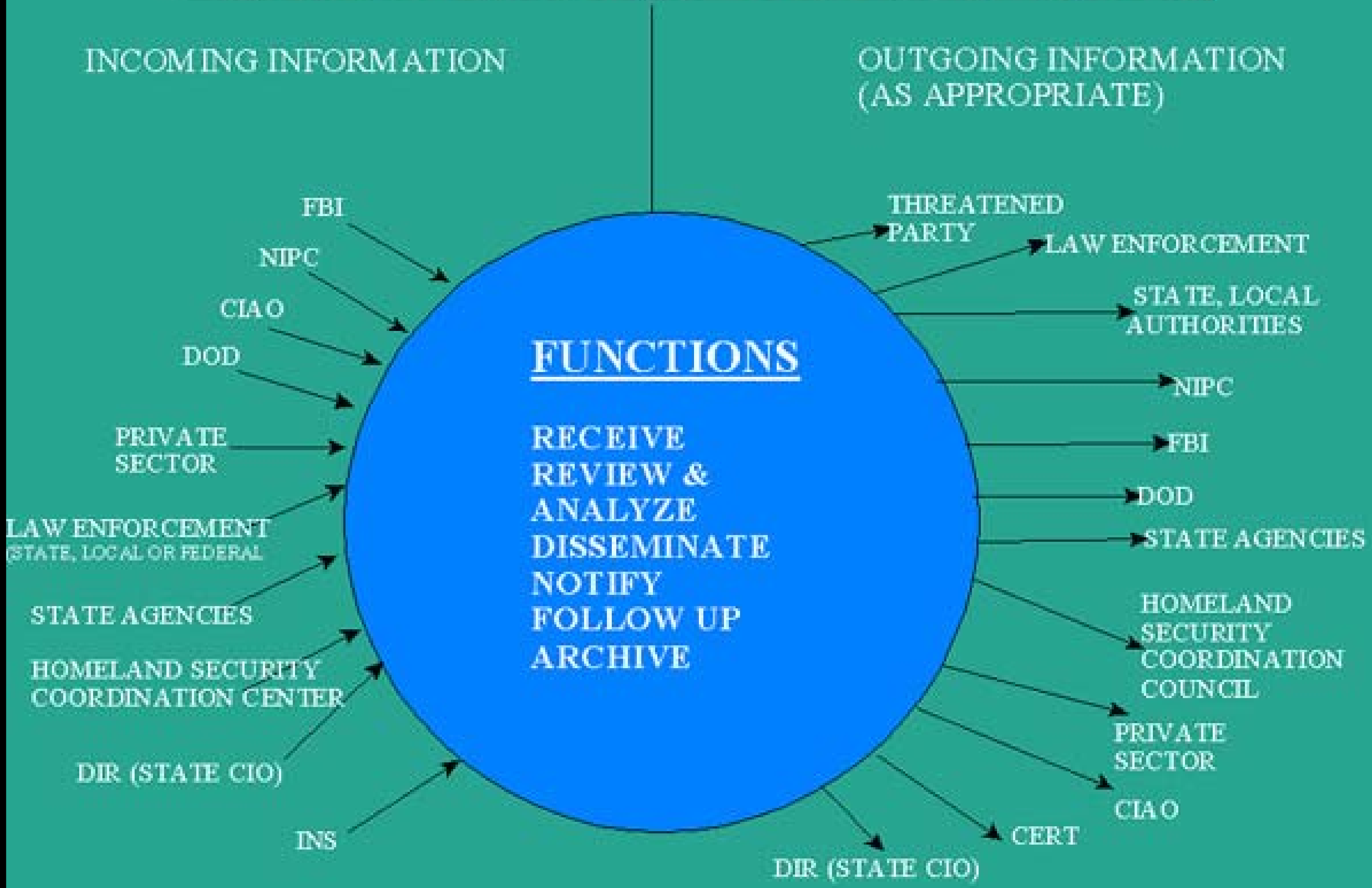
This includes public and private physical systems and cyber-systems essential to the minimum operations of the economy and state government including telecommunications, energy, banking, finance, transportation, water and emergency services.

Provide a state focal point for gathering information on threats to the information infrastructures.

Provide the principal means of facilitating and coordinating the state government's response to an incident, investigating incidents, mitigating attacks, investigating threats and monitoring reconstitution efforts.

Assist state agencies in the implementation of best practices for both physical assurance and information assurance

INFORMATION SHARING CENTER



INCOMING INFORMATION

FBI

NIPC

CIAO

DOD

PRIVATE SECTOR

LAW ENFORCEMENT (STATE, LOCAL OR FEDERAL

STATE AGENCIES

HOMELAND SECURITY COORDINATION CENTER

DIR (STATE CIO)

INS

FUNCTIONS

RECEIVE
REVIEW &
ANALYZE
DISSEMINATE
NOTIFY
FOLLOW UP
ARCHIVE

OUTGOING INFORMATION (AS APPROPRIATE)

THREATENED PARTY

LAW ENFORCEMENT

STATE, LOCAL AUTHORITIES

NIPC

FBI

DOD

STATE AGENCIES

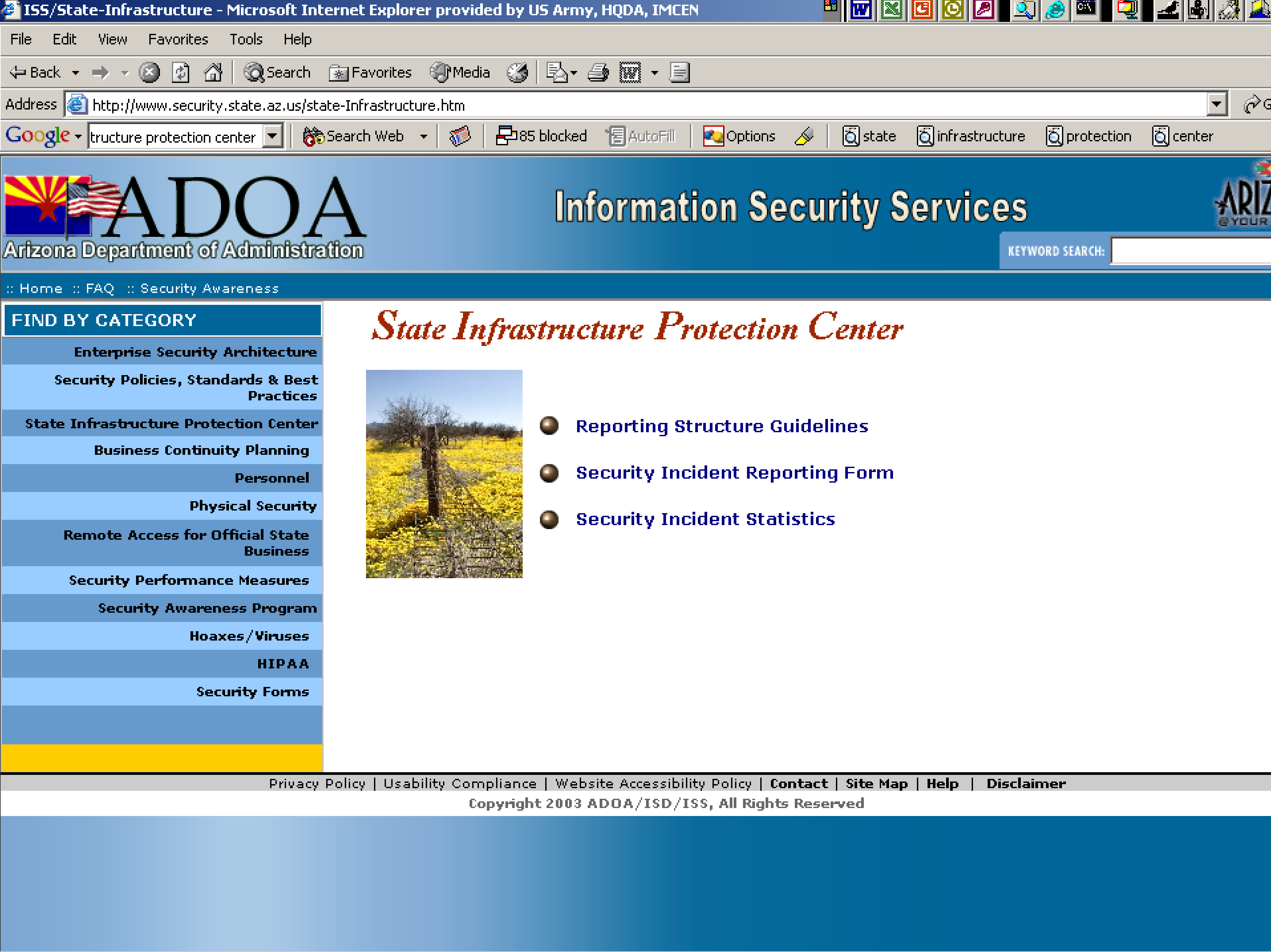
HOMELAND SECURITY COORDINATION COUNCIL

PRIVATE SECTOR

CIAO

CERT

DIR (STATE CIO)



ISS/State-Infrastructure - Microsoft Internet Explorer provided by US Army, HQDA, IMCEN
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.security.state.az.us/state-Infrastructure.htm
Google tructure protection center Search Web 85 blocked AutoFill Options state infrastructure protection center

ADOA
Arizona Department of Administration

Information Security Services

:: Home :: FAQ :: Security Awareness

FIND BY CATEGORY

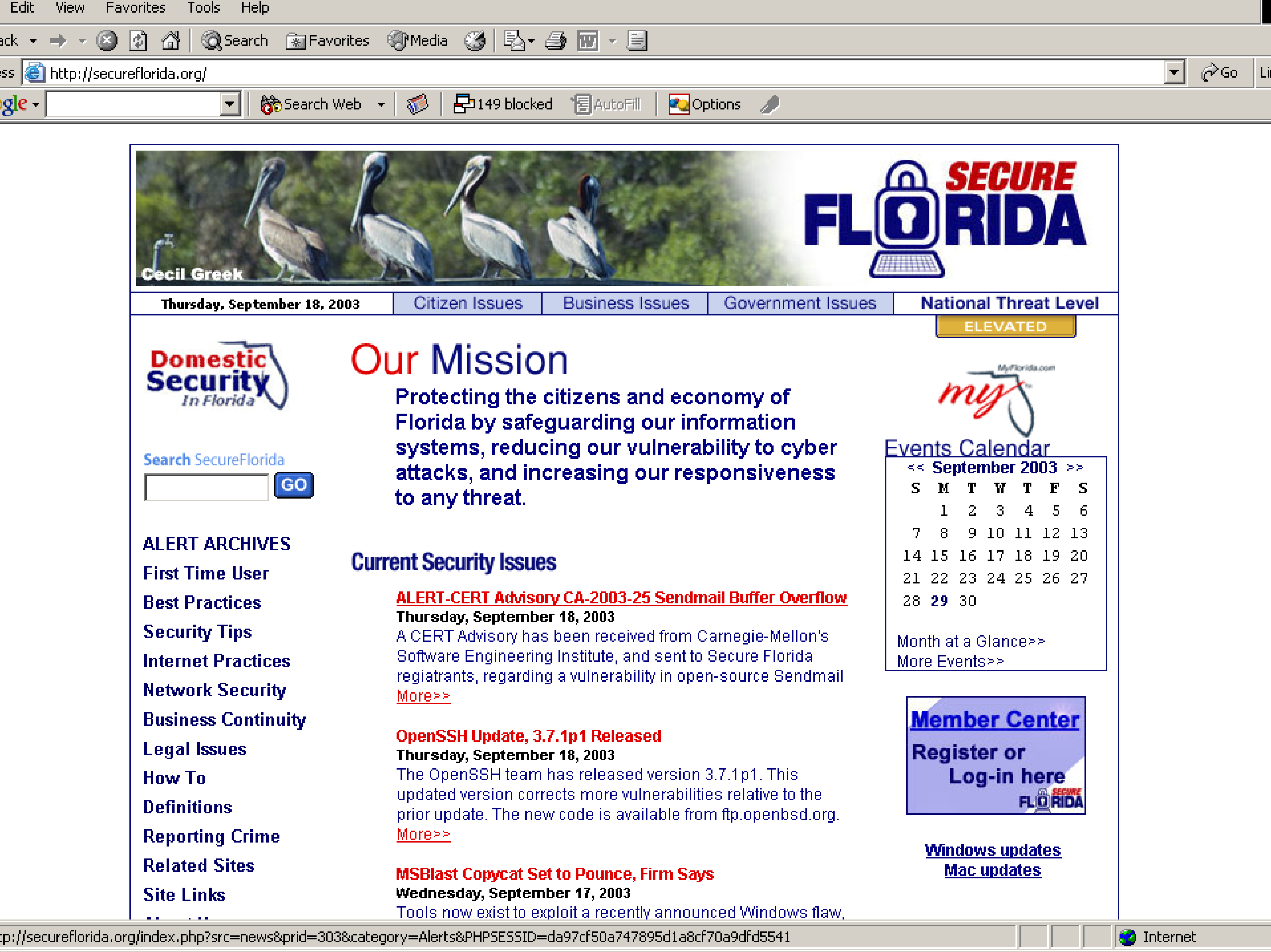
- Enterprise Security Architecture
- Security Policies, Standards & Best Practices
- State Infrastructure Protection Center
- Business Continuity Planning
- Personnel
- Physical Security
- Remote Access for Official State Business
- Security Performance Measures
- Security Awareness Program
- Hoaxes/Viruses
- HIPAA
- Security Forms

State Infrastructure Protection Center

- Reporting Structure Guidelines
- Security Incident Reporting Form
- Security Incident Statistics

Privacy Policy | Usability Compliance | Website Accessibility Policy | Contact | Site Map | Help | Disclaimer

Copyright 2003 ADOA/ISD/ISS, All Rights Reserved



Thursday, September 18, 2003 | Citizen Issues | Business Issues | Government Issues | National Threat Level

Domestic Security In Florida

Search SecureFlorida

ALERT ARCHIVES
First Time User
Best Practices
Security Tips
Internet Practices
Network Security
Business Continuity
Legal Issues
How To
Definitions
Reporting Crime
Related Sites
Site Links

Our Mission

Protecting the citizens and economy of Florida by safeguarding our information systems, reducing our vulnerability to cyber attacks, and increasing our responsiveness to any threat.

Current Security Issues

ALERT-CERT Advisory CA-2003-25 Sendmail Buffer Overflow
Thursday, September 18, 2003
A CERT Advisory has been received from Carnegie-Mellon's Software Engineering Institute, and sent to Secure Florida regiatrants, regarding a vulnerability in open-source Sendmail
More>>

OpenSSH Update, 3.7.1p1 Released
Thursday, September 18, 2003
The OpenSSH team has released version 3.7.1p1. This updated version corrects more vulnerabilities relative to the prior update. The new code is available from ftp.openbsd.org.
More>>

MSBlast Copycat Set to Pounce, Firm Says
Wednesday, September 17, 2003
Tools now exist to exploit a recently announced Windows flaw,

Events Calendar

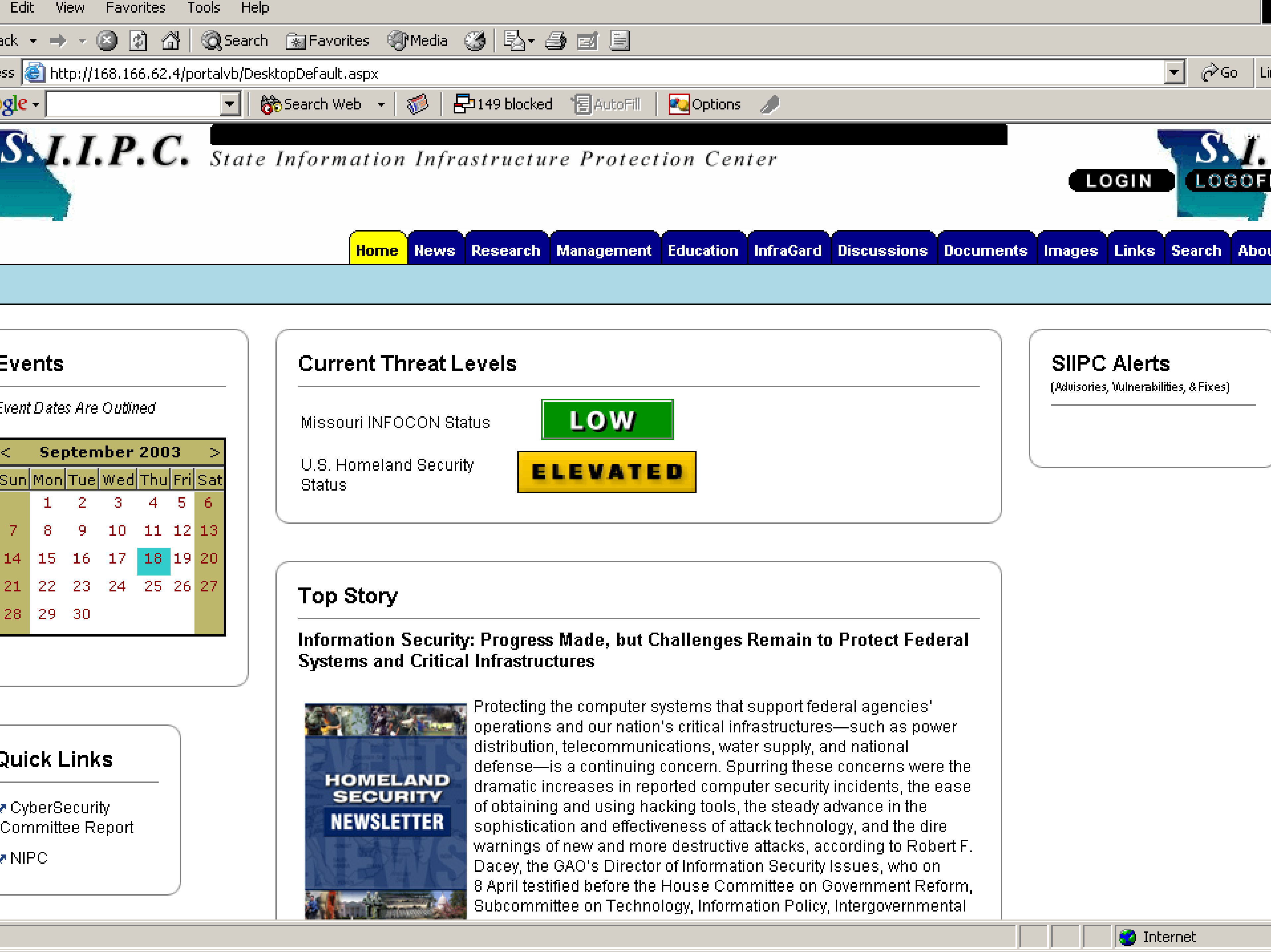
<< September 2003 >>

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	**29**	30				

Month at a Glance>>
More Events>>

Windows updates
Mac updates

p://secureflorida.org/index.php?src=news&prid=303&category=Alerts&PHPSESSID=da97cf50a747895d1a8cf70a9dfd5541



S.I.I.P.C.

[redacted]

State Information Infrastructure Protection Center

Events

Event Dates Are Outlined

<	September 2003					>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Quick Links

- CyberSecurity Committee Report
- NIPC

Current Threat Levels

Missouri INFOCON Status	LOW
U.S. Homeland Security Status	ELEVATED

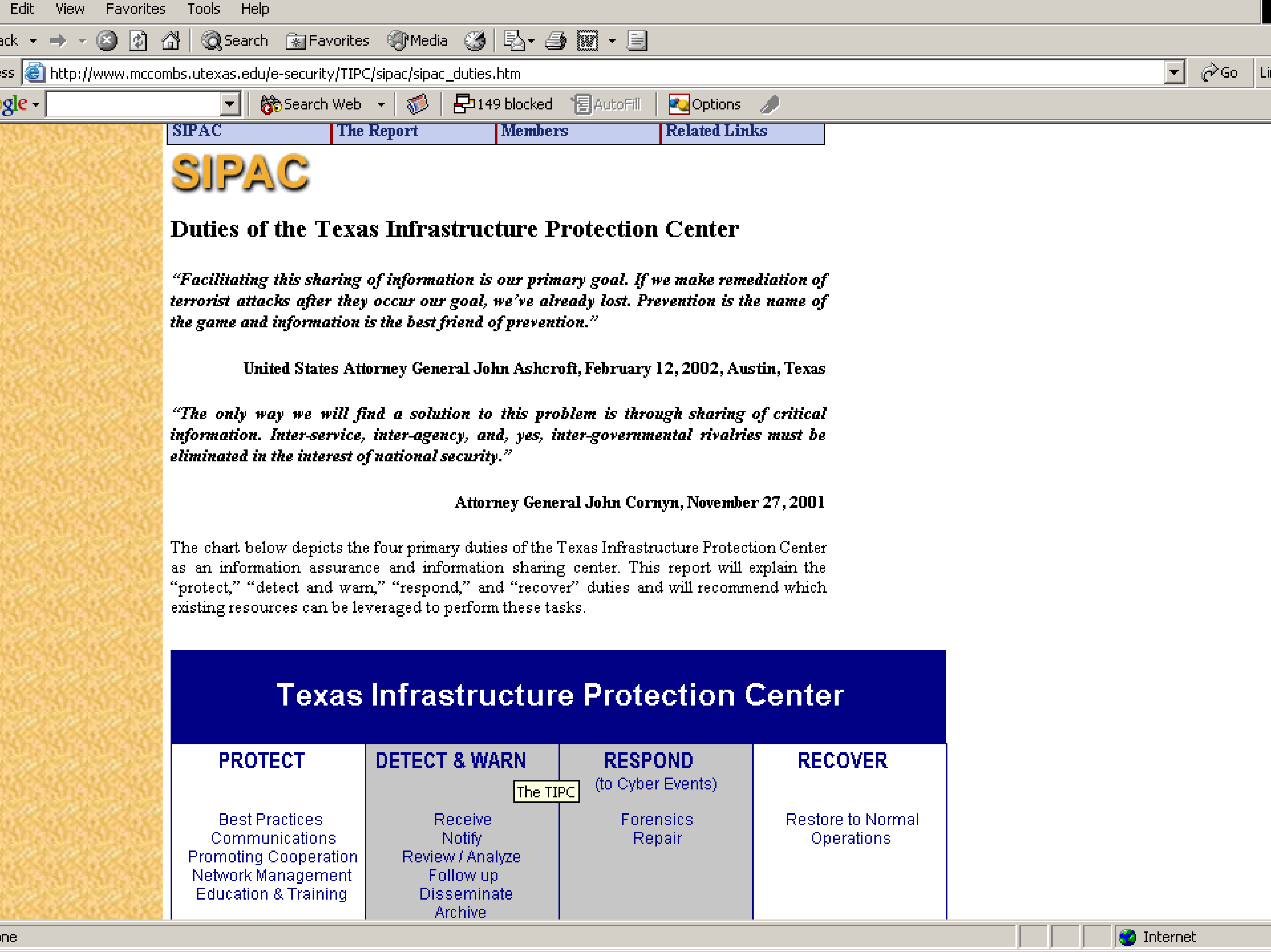
SIIPC Alerts

(Advisories, Vulnerabilities, & Fixes)

Top Story

Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and Critical Infrastructures

Protecting the computer systems that support federal agencies' operations and our nation's critical infrastructures—such as power distribution, telecommunications, water supply, and national defense—is a continuing concern. Spurring these concerns were the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks, according to Robert F. Dacey, the GAO's Director of Information Security Issues, who on 8 April testified before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental


Edit View Favorites Tools Help
ack
Search
Favorites
Media
http://www.mccombs.utexas.edu/e-security/TIPC/sipac/sipac_duties.htm
Go
gle
Search Web
149 blocked
AutoFill
Options
one
Internet

SIPAC | The Report | Members | Related Links

SIPAC

Duties of the Texas Infrastructure Protection Center

"Facilitating this sharing of information is our primary goal. If we make remediation of terrorist attacks after they occur our goal, we've already lost. Prevention is the name of the game and information is the best friend of prevention."

United States Attorney General John Ashcroft, February 12, 2002, Austin, Texas

"The only way we will find a solution to this problem is through sharing of critical information. Inter-service, inter-agency, and, yes, inter-governmental rivalries must be eliminated in the interest of national security."

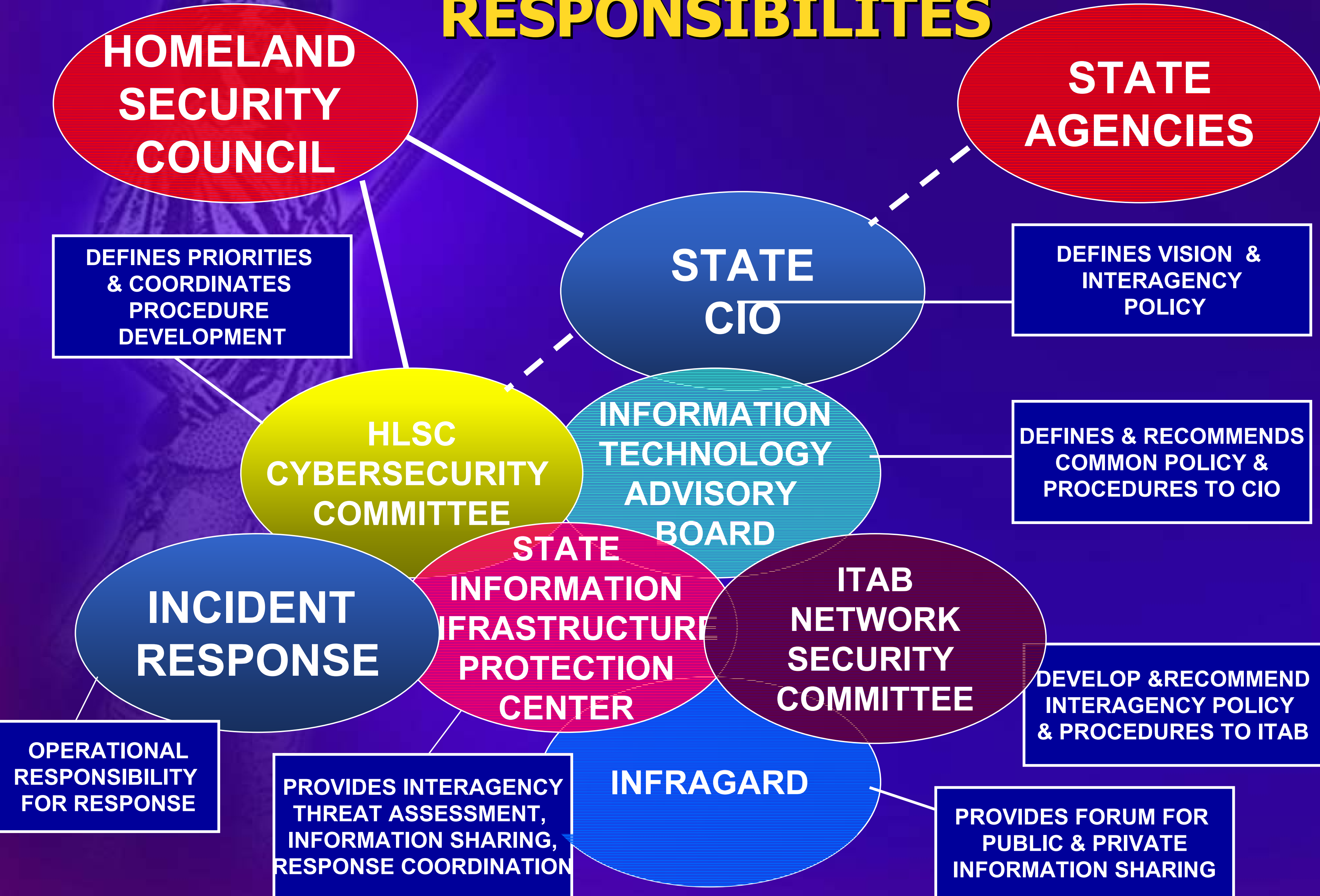
Attorney General John Cornyn, November 27, 2001

The chart below depicts the four primary duties of the Texas Infrastructure Protection Center as an information assurance and information sharing center. This report will explain the "protect," "detect and warn," "respond," and "recover" duties and will recommend which existing resources can be leveraged to perform these tasks.

Texas Infrastructure Protection Center

PROTECT	DETECT & WARN	RESPOND (to Cyber Events)	RECOVER
Best Practices Communications Promoting Cooperation Network Management Education & Training	Receive Notify Review / Analyze Follow up Disseminate Archive	Forensics Repair	Restore to Normal Operations

CYBERSECURITY ROLES AND RESPONSIBILITES



HOMELAND SECURITY COUNCIL

DEFINES PRIORITIES & COORDINATES PROCEDURE DEVELOPMENT

STATE AGENCIES

STATE CIO

DEFINES VISION & INTERAGENCY POLICY

HLSC CYBERSECURITY COMMITTEE

INFORMATION TECHNOLOGY ADVISORY BOARD

DEFINES & RECOMMENDS COMMON POLICY & PROCEDURES TO CIO

INCIDENT RESPONSE

OPERATIONAL RESPONSIBILITY FOR RESPONSE

STATE INFORMATION INFRASTRUCTURE PROTECTION CENTER

PROVIDES INTERAGENCY THREAT ASSESSMENT, INFORMATION SHARING, RESPONSE COORDINATION

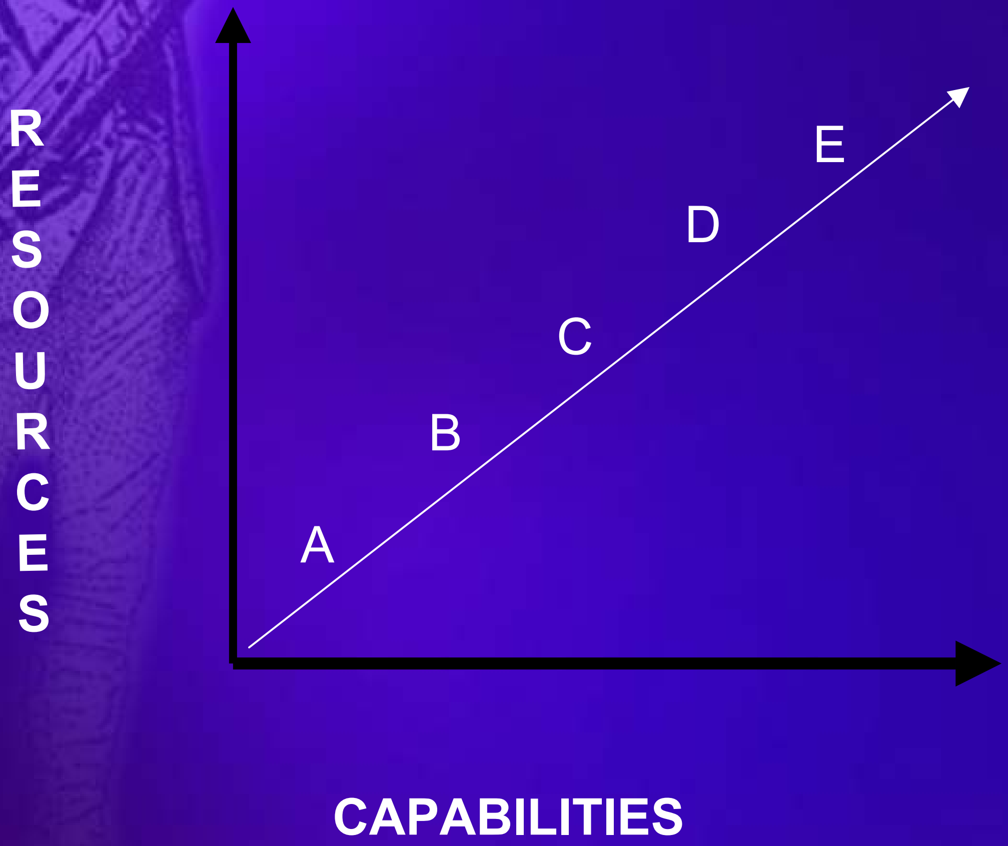
ITAB NETWORK SECURITY COMMITTEE

DEVELOP &RECOMMEND INTERAGENCY POLICY & PROCEDURES TO ITAB

INFRAGARD

PROVIDES FORUM FOR PUBLIC & PRIVATE INFORMATION SHARING

Possible Implementation Models



E= 24x7 Professional Staff with analysis and reporting capability

D= 24x7 CERT w/ VAT

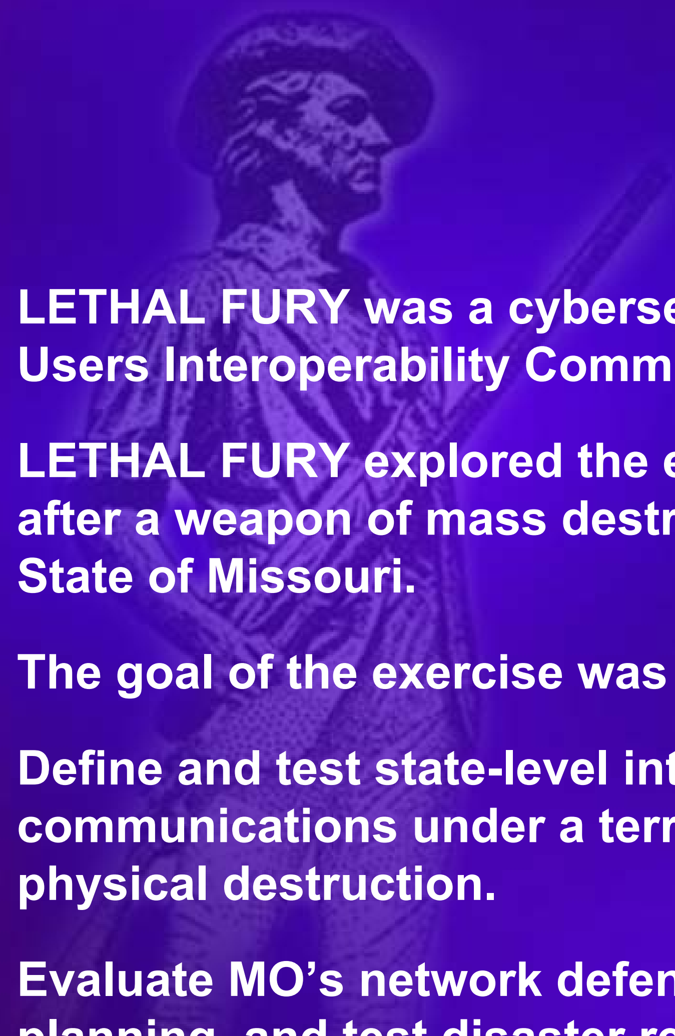
C= 5x10 CERT Staff

B= Email with on-call support

A= Automatic email notification

Cyber Exercise Development

LETHAL FURY



LETHAL FURY was a cybersecurity exercise conducted as part of the Joint Users Interoperability Communications Exercise (JUICE) 2003.

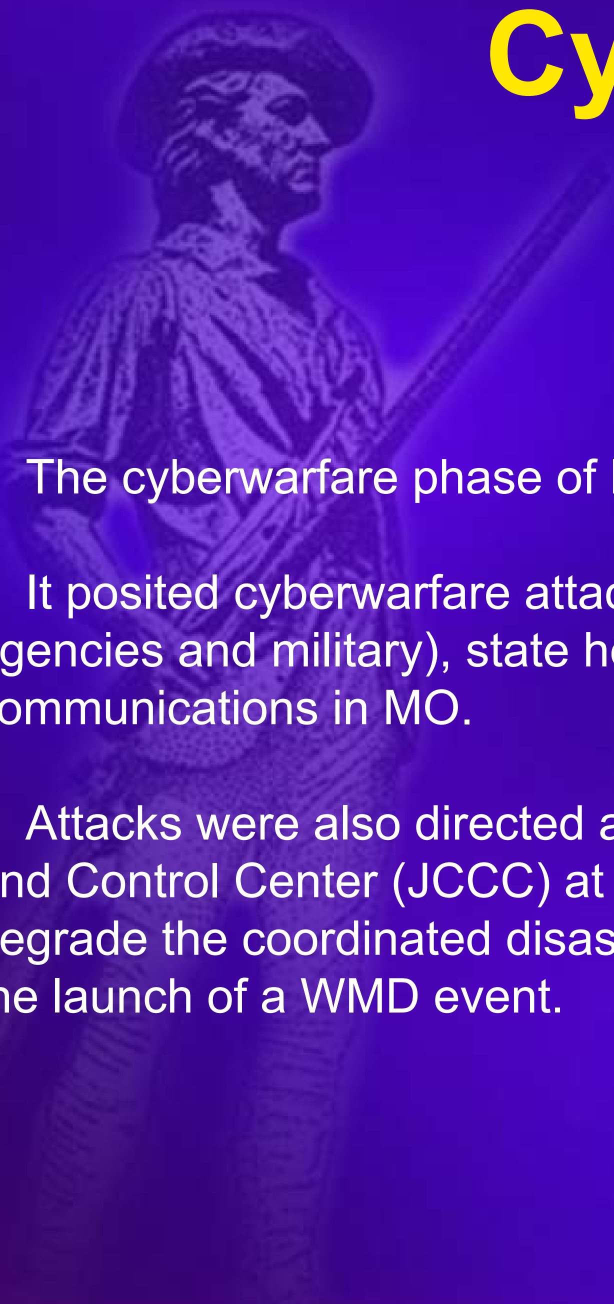
LETHAL FURY explored the effects of cyberwarfare attacks before, during, and after a weapon of mass destruction attack on critical infrastructures within the State of Missouri.

The goal of the exercise was two-fold.

Define and test state-level interagency, federal interagency, and DoD multi-user communications under a terrorism scenario involving both cyber-attack and physical destruction.

Evaluate MO’s network defense/cybersecurity capabilities, business continuity planning, and test disaster response communications interoperability.

Participating agencies validated efforts to support critical infrastructure protection through Missouri’s newly created State Information Infrastructure Protection Center (SIIPC).



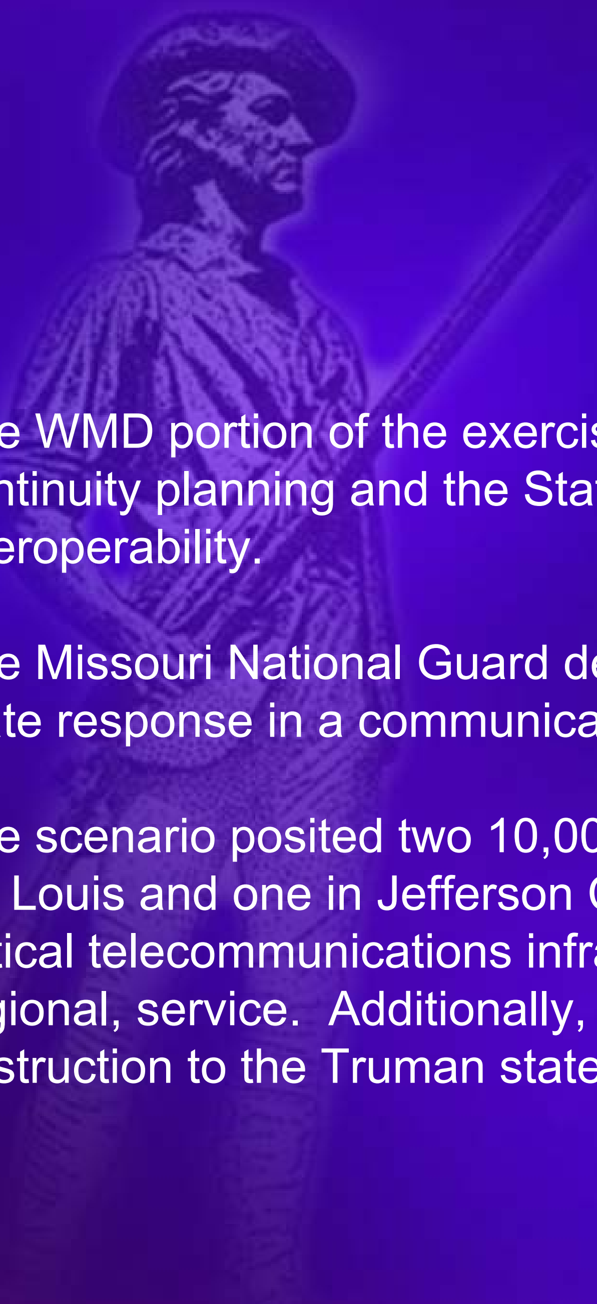
Cyberwarfare Phase

The cyberwarfare phase of LETHAL FURY took place over a three-day period.

It posited cyberwarfare attacks against critical state infrastructures (government agencies and military), state health care systems, and first responder communications in MO.

Attacks were also directed against a simulated Joint Task Force Joint Command and Control Center (JCCC) at Fort Monmouth, NJ. The goal of the attacks was to degrade the coordinated disaster response capabilities of state critical assets prior to the launch of a WMD event.

WMD Phase

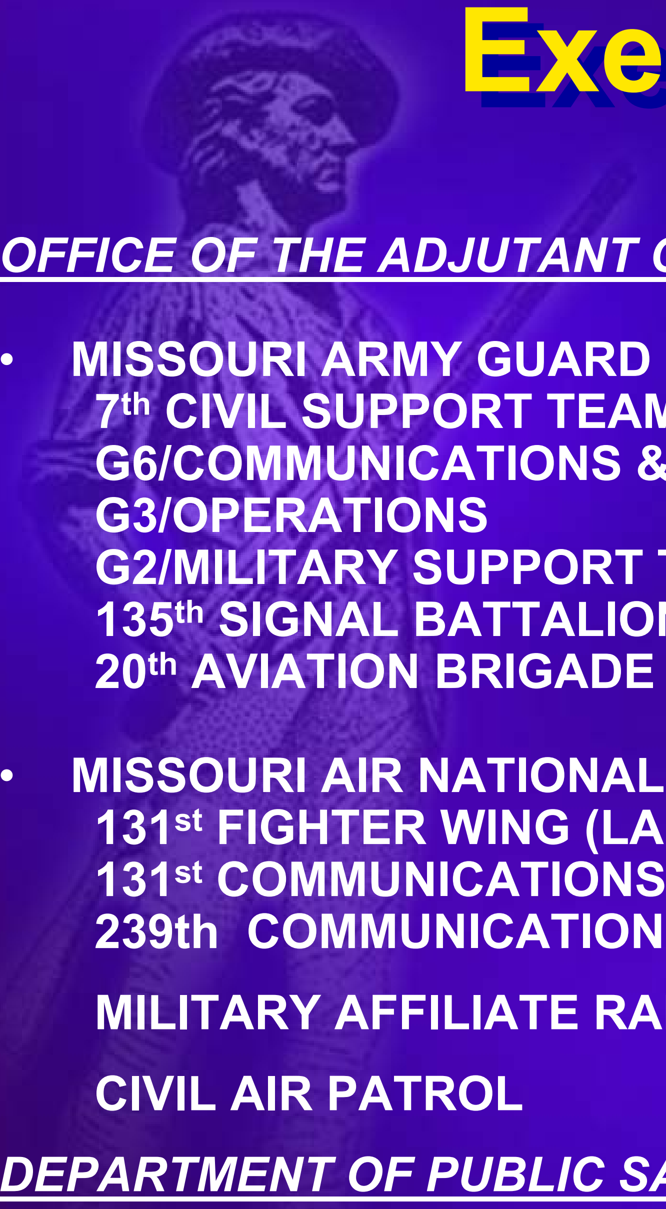


The WMD portion of the exercise tested the Missouri National Guard’s business continuity planning and the State’s disaster response communications interoperability.

The Missouri National Guard developed a scenario that would require a multi-agency state response in a communications degraded environment.

The scenario posited two 10,000-pound ammonium nitrate-fuel oil explosives, one in St. Louis and one in Jefferson City. Both devices were located so as to damage critical telecommunications infrastructures so as to break down local, and potentially regional, service. Additionally, the Jefferson City device would create considerable destruction to the Truman state office building.

Exercise Participants



OFFICE OF THE ADJUTANT GENERAL

- MISSOURI ARMY GUARD
  7th CIVIL SUPPORT TEAM
  G6/COMMUNICATIONS & INFORMATION
  G3/OPERATIONS
  G2/MILITARY SUPPORT TO CIVILIAN AUTHORITIES
  135th SIGNAL BATTALION
  20th AVIATION BRIGADE

- MISSOURI AIR NATIONAL GUARD
  131st FIGHTER WING (LAMBERT)
  131st COMMUNICATIONS FLIGHT (JEFFERSON BARRACKS)
  239th COMMUNICATIONS FLIGHT (ROSECRANTZ)

MILITARY AFFILIATE RADIO SYSTEM (MARS)

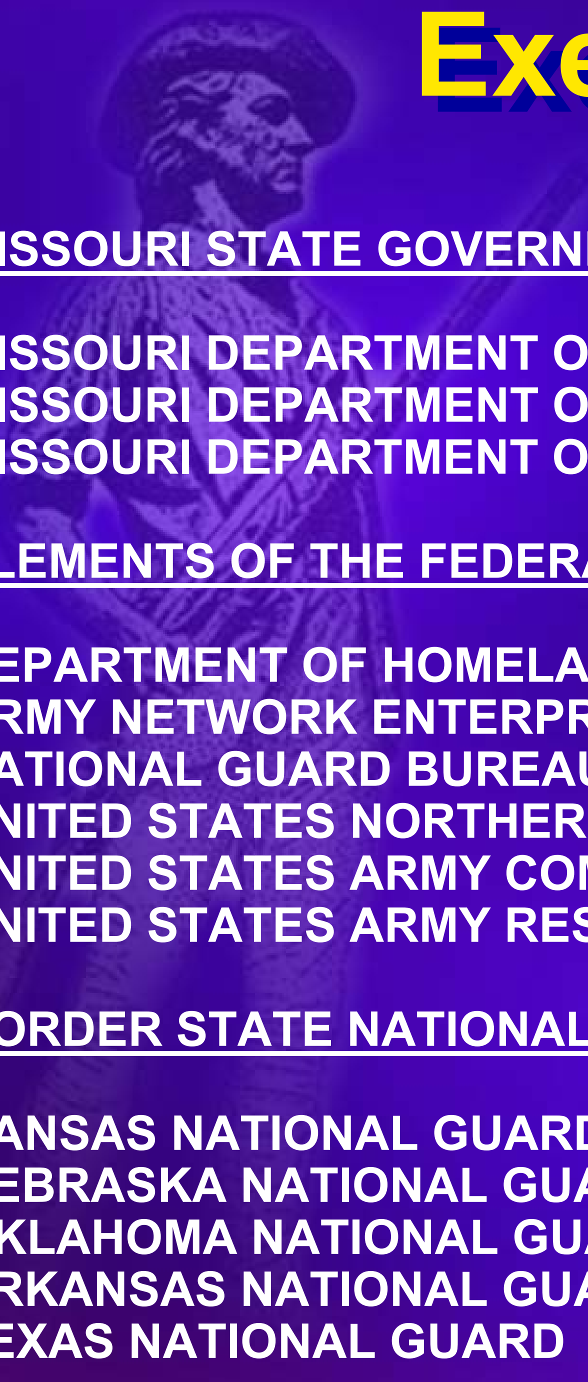
CIVIL AIR PATROL

DEPARTMENT OF PUBLIC SAFETY

MISSOURI STATE HIGHWAY PATROL

STATE EMERGENCY MANAGEMENT AGENCY

Exercise Participants



MISSOURI STATE GOVERNMENT

MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES
MISSOURI DEPARTMENT OF AGRICULTURE
MISSOURI DEPARTMENT OF TRANSPORTATION

ELEMENTS OF THE FEDERAL GOVERNMENT

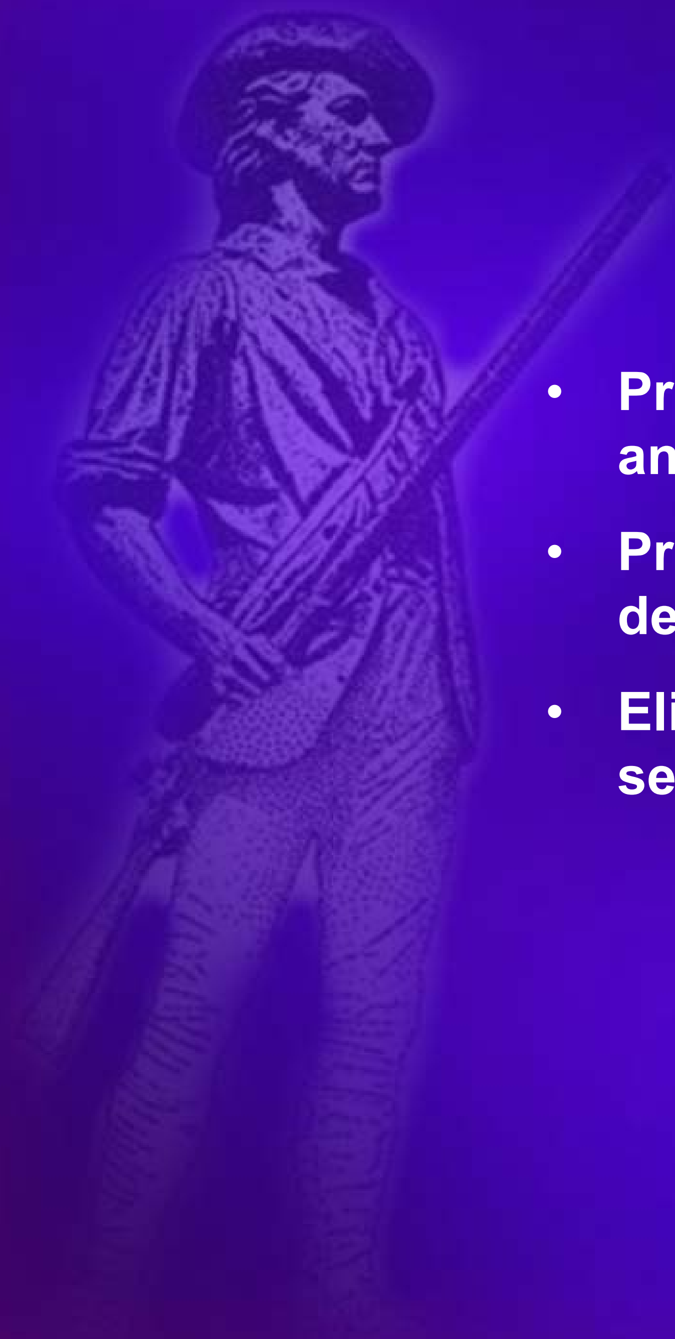
DEPARTMENT OF HOMELAND SECURITY/FEMA (OBSERVERS)
ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND
NATIONAL GUARD BUREAU (OBSERVERS)
UNITED STATES NORTHERN COMMAND (OBSERVERS)
UNITED STATES ARMY COMMUNICATIONS ELECTRONICS COMMAND
UNITED STATES ARMY RESERVE INOFRMAITON OPERATIONS COMMAND

BORDER STATE NATIONAL GUARD ELEMENTS (OBSERVERS)

KANSAS NATIONAL GUARD
NEBRASKA NATIONAL GUARD
OKLAHOMA NATIONAL GUARD
ARKANSAS NATIONAL GUARD
TEXAS NATIONAL GUARD

KENTUCKY NATIONAL GUARD
TENNESSEE NATIONAL GUARD
ILLINOIS NATIONAL GUARD
IOWA NATIONAL GUARD

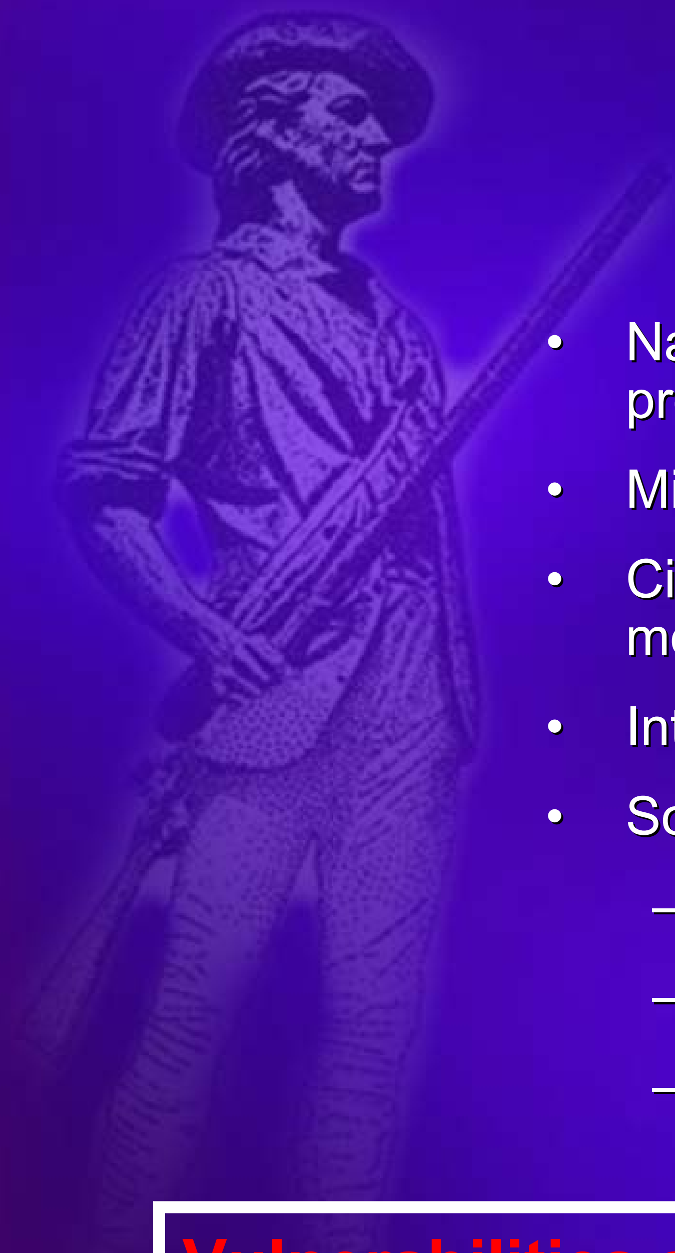
Conclusion



Key ISIP Benefits

- Provides a reliable comprehensive, scalable, and timely security resource
- Provides information on multiple levels from decision makers to technicians
- Eliminates costly search for cyber security solutions

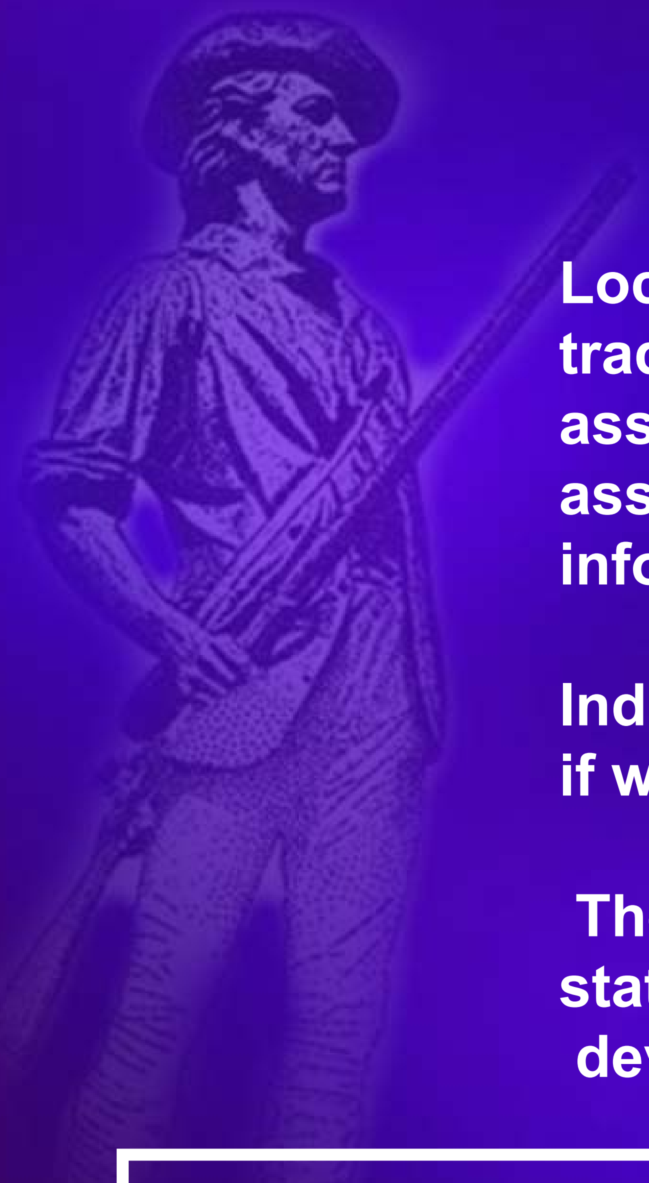
Why ISIP?



- National military strategy is dependent on force projection
- Military mobilization is essential to force projection
- Civil/private sectors control resources that impact mobilization
- Interdependencies exist
- Solutions and best practices exist
  - Identification
  - Dissemination
  - Reporting

Vulnerabilities are shared and interdependent

Conclusion



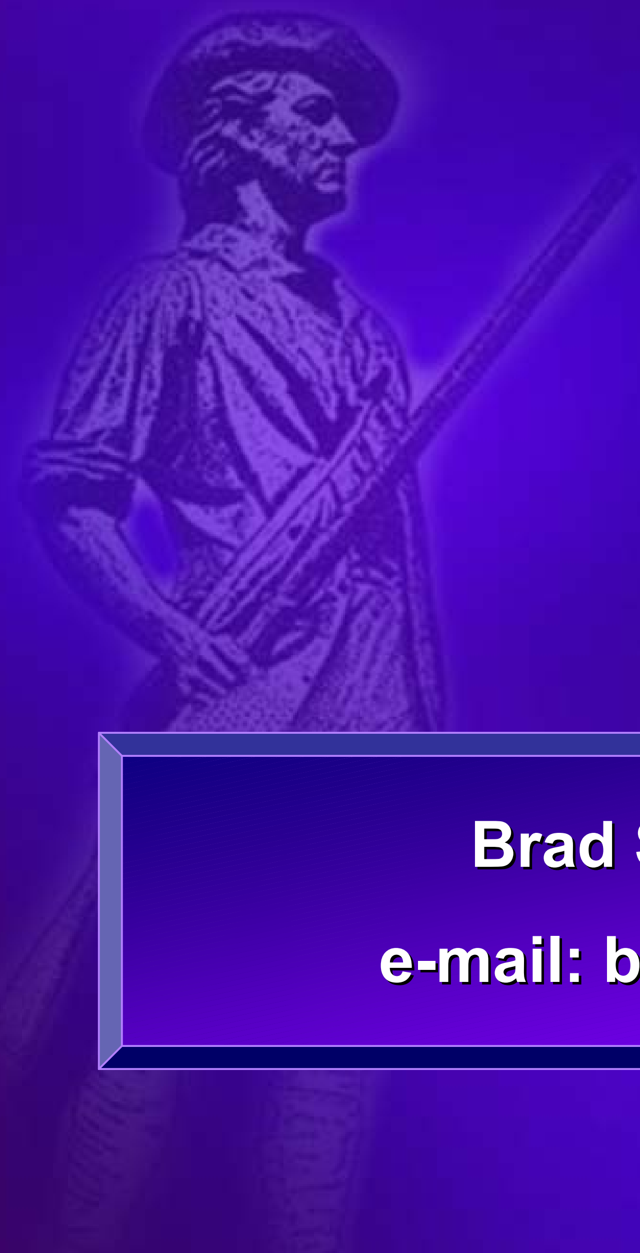
Local and state governments have not traditionally had the responsibility or the assets needed to provide information assurance protection for their critical information infrastructures.

Industry must become a partner in this effort if we are to be successful.

The DoD and DA are willing to assist the states to
develop these capabilities.

ISIP will add significant value to DoD mission integrity and Homeland Security

ISIP Contact



Brad Shere (703) 604-7584

e-mail: bradley.shere@us.army.mil

http://www.army.mil/ciog6/isip/